

양자암호통신 기술

Quantum Cryptography

정보통신 미래기술 특집

노태곤 (T.-G. Noh)	신기능정보소자팀 선임연구원
김현오 (H. Kim)	신기능정보소자팀 선임연구원
홍종렬 (J. Hong)	신기능정보소자팀 선임연구원
윤천주 (C. J. Youn)	신기능정보소자팀 선임연구원
성건용 (G. Y. Sung)	신기능정보소자팀 팀장
정태혁 (T. Zyung)	미래기술연구본부 본부장

목 차

- I. 서론
- II. 양자암호 프로토콜과 안전성
- III. 양자암호통신 구현기술
- IV. 결론

양자암호통신 기술은 통신상의 보안을 자연의 기본원리인 양자역학의 법칙에 의해서 보장하므로 도청이나 감청이 절대적으로 불가능한 차세대 통신보안 기술로서 최근 크게 주목받고 있다. 즉, 양자암호통신 기술은 “양자 복제불가능성”과 같은 양자물리학의 법칙에 기초해서 송신자와 수신자 사이에 암호 키(일회용 난수표)를 절대적으로 안전하게 실시간으로 분배하는 기술로서 “양자 키 분배 기술”로도 알려져 있다. 본 고에서는 이러한 양자암호통신 기술의 기본원리 및 구현기술의 개요와 그 연구개발 동향에 대해서 기술한다.

I. 서론

인터넷을 비롯한 유무선 통신의 사용이 급속히 확대됨에 따라 통신네트워크의 보안문제는 국가, 기업, 금융상의 중요기밀 보호 및 개인의 사생활 보호 측면에서 그 중요성이 점점 더 중대되고 있다. 1970년대에 개발되어 현재 인터넷 등 통신시스템에 널리 사용되고 있는 비대칭 공개키 암호체계는 해결하기 매우 어려운 수학적인 문제를 공개키로 사용하여 정보를 암호화하고 그 해를 비밀키로 사용하여 해독하는 방식으로서 원리적으로 수학적인 “계산 복잡성”에 기초하고 있다[1]. 대표적으로 Rivest, Shamir, Adleman 등 세 사람이 개발한 RSA 공개키 암호체계는 매우 큰 수를 소인수분해하기가 매우 난해하다는 점을 이용한다. 즉, 수학적으로 소인수분해 문제는 문제의 크기가 증가함에 따라 계산시간이 지수함수적으로 증가하게 되며 따라서 송신자와 수신자가 충분히 큰 숫자의 소인수분해 문제를 공개키로 사용하면 도청자가 암호문을 해독하기는 현실적으로 불가능 할 것이라는 점을 이용한다. 그러나, 이러한 수학적인 계산복잡성에 기초한 암호체계는 보다 정교한 알고리듬의 발전에 따라 그 안전성이 의문이 제기되고 있으며, 또한 1994년 AT&T의 Peter Shor가 양자컴퓨터를 이용한 소인수분해 알고리듬을 개발함으로써 양자컴퓨터가 개발되면 RSA 암호체계는 근본적으로 해독이 가능한 것으로 판명되고 있다[2]. 이러한 보안문제를 해결할 대안으로 등장한 양자암호통신(quantum cryptography) 기술은 그 안전성이 수학적인 계산 복잡성이 아닌 자연의 근본 법칙인 양자역학의 원리에 기초하므로 도청 및 감청이 근본적으로 불가능하며 그 안전성이 절대적으로 보장된다[3].

본 고에서 기술하는 양자암호통신 기술은 보다 넓은 의미에서 디지털 정보기술의 외연을 양자물리학으로 확장한 양자정보 기술(quantum information technology)의 한 분야이다. 1980년대 중반부터 본격적으로 연구되기 시작한 양자정보처리 및 양자정보통신 기술은 양자암호통신 기술을 비롯하여

원거리에 양자상태를 순간적으로 이동하는 양자원격전송 기술, 그리고 ‘양자 중첩’ 및 ‘양자 얹힘’의 원리를 응용하여 기존 컴퓨터 기술로는 불가능한 대규모 계산을 가능하게 하는 양자계산과 초고속 데이터 검색 기술 등의 다양한 정보기술로 급속하게 발전하고 있다[4]. 즉, 기존의 정보처리 및 통신 기술과 비교해서 양자정보기술은 정보를 양자상태에 직접적으로 표현하고 처리함으로써 기존의 기술로는 불가능하다고 생각되는 다양한 일들을 수행할 수 있다.

이와 같이 기존 정보기술에 패러다임의 변화를 가져올 혁명적인 양자정보 기술 중에서도 특히 양자암호통신 기술은 가장 기초적이고 또한 기술성숙도가 가장 높은 기술로서 현재 미국, 유럽, 일본 등 선진국을 중심으로 세계적으로 활발한 연구가 이루어지고 있다. 미국의 경우 CIA, NSA, NASA 등의 국가 안보 관련 기관을 중심으로 유럽의 경우에는 유럽 공동체 차원의 연구 지원이 이루어지고 있다. 특히, 최근에는 세계적인 기업들의 관련 연구활동이 증가하고 있는 추세이며, IBM, HP, Bell Lab., Fujitsu, NEC, NTT, Toshiba, Mitsubishi 등 기업연구소에서도 주목할 만한 연구결과를 발표하고 있다. 또한, 양자암호통신 기술은 기술적인 측면에서 기존의 광통신기술을 활용하여 통신 사업자들이 기 매설한 광섬유시설을 곧바로 이용 가능하므로 머지 않은 시점에 대규모 상용화가 가능할 것이라는 것이 대체적인 의견이다. 실제로 2002년 스위스 id Quantique사와 2003년 미국 MagiQ Technologies사에서 각각 초보적인 수준의 상용시스템을 발표하는 등 상용화 전 단계까지 발전하고 있다. 우리나라의 경우에는 양자암호이론분야는 몇몇 연구기관을 중심으로 상당한 수준의 연구들을 진행하고 있으나 실험적인 구현연구는 연구투자 및 성과가 아직 선진국에 비해 크게 미흡한 상태에 있다.

본 고에서는 이와 같이 통신네트워크의 보안문제에 근본적인 해결책을 제시하는 양자암호통신 기술의 기본적인 원리 및 실제 구현과 관련된 재반 기술의 개요와 동향에 대해서 기술한다.

II. 양자암호 프로토콜과 안전성

앞에서 언급한 RSA 암호체계와 같은 비대칭 공개키 암호체계와 달리 송신자와 수신자가 일회용 난수표(one-time pad)를 서로 나누어 가진 후 이것을 암호 키로 사용하는 대칭암호체계는 절대적인 안전성이 보장된다. 문제는 이러한 일회용 난수표를 실시간으로 안전하게 나누어 가지는 방법이다. 양자암호통신 기술은 이러한 일회용 난수표를 양자 복제를 가능성[5]과 같은 양자물리학의 법칙에 기초해서 실시간으로 송신자와 수신자 사이에 안전하게 분배하는 기술로서 “양자 키 분배(QKD)” 기술로도 불린다.

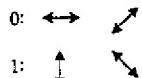
양자암호 프로토콜과 관련된 이론연구는 크게 두 가지 영역에서 이루어지고 있다. 그 중 하나는 새로운 양자암호 프로토콜의 창안이고, 다른 하나는 창안된 프로토콜의 안전성 증명에 대한 연구이다. 물론 이 두 영역의 연구는 전혀 별개의 것이 아니므로 새로운 프로토콜을 제안하는 경우 그 프로토콜의 안전성을 증명하는 것이 병행되는 것이 보통이며, 또한 기존의 프로토콜에 대한 공격 방법 제시와 그 공격에 대비해 프로토콜을 변형하여 새로운 프로토콜을 제안하는 방향으로 연구가 진행되는 경우도 많다. 본 절에서는 지금까지 제안된 양자암호 프로토

콜들의 기본 개념과 그 프로토콜들에 대해 제안된 다양한 공격방법, 그리고 안전성 증명에 대한 연구 동향을 기술한다.

1. 양자암호 프로토콜

최초의 양자 암호 프로토콜은 1984년 IBM의 C. H. Bennett과 몬트리올 대학의 G. Brassard에 의해 발표되었다[6]. 고안자들의 이름을 따서 BB84 프로토콜로 명명된 이 프로토콜은 (그림 1)에서 보는 것과 같이 두 개의 기저(basis)를 이루는 네 개의 양자 상태(예를 들면, 단일광자의 편광상태)를 이용한다.

즉, 송신자(Alice)는 두 개의 기저, 즉 \leftrightarrow 혹은 \times 중에서 한 개를 무작위로 선택하고(1단계), 선택된 기저의 두 가지 양자상태(암호 키 값), 즉 0 혹은 1 중에서 하나를 임의로 골라 수신자(Bob)에게 보낸다(2단계). 양자상태를 수신하는 Bob도 역시 두 가지 기저 중 하나를 무작위로 선택하고(3단계), 선택한 기저를 사용하여 수신된 양자상태를 측정한다(4단계). Bob의 측정이 끝난 뒤 Alice와 Bob은 자신들이 임의로 선택한 기저를 서로에게 공개하는데, Alice가 선택한 기저와 Bob이 선택한 기저가 같은

1단계: Alice-basis 선택		\leftrightarrow	\times	\times	\leftrightarrow	\times	\leftrightarrow	\times	\leftrightarrow
2단계: Alice-암호 키 값 선택		1	0	1	1	0	0	0	0
Eve의 도청 시도	Eve-basis 선택	-	-	-	-	\times	\times	-	-
	Eve-도청한 정보	-	-	-	-	0	1	-	-
3단계: Bob-basis 선택		\leftrightarrow	\times	\leftrightarrow	\times	\times	\leftrightarrow	\leftrightarrow	\leftrightarrow
4단계: Bob-암호 키 값 측정		1	0	1	0	0	1	0	0
5단계: Basis 비교-sifted key		○	○	-	-	○	○	-	○
암호 키 값에 대응하는 양자상태									
0: 									
1: 									



(그림 1) BB84 프로토콜과 차단-재송신 도청공격

경우 Bob이 측정한 결과는 Alice가 임의로 고른 양자 상태와 일치하며, 따라서 두 사용자가 같은 암호 키(sifted key)를 가지게 된다(5단계). (그림 1)에서 보듯이 만약 중간에 도청자(Eve)가 도청을 시도한다면 양자 역학의 기본 원리에 의해 두 사용자(Alice와 Bob)가 얻은 암호 키 값에 오류를 만들어내게 되며 Alice와 Bob은 생성된 키의 일부를 서로에게 공개해서 오류의 비율을 계산하여 Eve의 존재 여부를 알게 되는 것이다.

한편, 1992년 C.H. Bennett은 서로 직교하지 않는 두 개의 양자상태만 있으면 양자암호통신을 구현하는 데 충분함을 보였다[7]. 이 프로토콜을 보통 B92라고 부른다. 이 프로토콜은 네 개의 상태를 사용하는 BB84에 비해 실제 실험에서 구현하기 쉽기 때문에 초기 양자 암호 실험에서 사용되었다. 일반적으로 두 개의 상태면 충분하고 네 개의 상태를 사용하는 프로토콜을 표준으로 생각하지만 양자상태가 존재하는 힐버트 공간에서의 대칭성을 생각하여 6개나 혹은 3개의 양자 상태를 사용하는 프로토콜도 발표되었다[8].

또한, Alice가 양자상태를 선택해 Bob에게 보내고 Bob은 그 양자상태를 측정하는 방식 외에도 두 사용자가 EPR 상태(최대 양자 얹힘상태)에 있는 두 개의 입자를 각각 한 개씩 나누어 가지고 각각의 입자에 대해 측정을 가하는 방식의 양자암호 프로토콜이 1991년 A. Ekert에 의해 발표되었다[9]. 이 프로토콜은 보통 E91프로토콜로 불리는데, 두 사용자는 두 개의 기저가 아닌 각각 세 개의 기저 중 하나를 선택해 그 기저에 의해 측정을 하게 된다. Alice의 세 기저와 Bob의 세 기저 중 두 기저는 일치하지만 나머지 하나의 기저는 서로 다르다. 따라서 두 사용자의 측정 기저가 동일하여 암호 키를 얻을 수 있는 확률은 $2/9$ 로 줄어들지만 나머지 기저가 일치하지 않는 값들로부터 Eve의 존재 등 안전성에 대한 평가를 동시에 할 수 있다. 이 안전성 평가는 소위 “벨 부등식”을 이용한 것인데 벨 부등식과 양자 암호에서의 안전성 사이의 관계에 대한 약간의 논쟁이 있었으며, 이 문제는 최근까지 연구 대상이 되고 있

다[10].

지금까지 언급한 양자 암호 프로토콜들은 차원이 2인 힐버트 공간의 양자계 즉, 큐빗(Qubit, 양자비트)을 이용하는 것이다. 이에 대한 확장으로 차원이 2보다 큰 양자계를 이용한 양자암호 프로토콜이 연구되었으며, 더 나아가 연속 변수로 구현하는 양자암호 프로토콜에 대한 연구에까지 이르렀다. 연속 변수 양자암호 프로토콜은 빛의 직교진폭(quadrature amplitude)을 암호 키 생성에 이용하는 것으로 압축광(squeezed light)이나, 간섭성광(coherent light)을 사용한다. 이러한 연속 변수 양자 암호 프로토콜 역시 실험적으로 구현되기도 했다[11]. 간섭성광의 고전적 잡음을 이용해 양자 암호에 필적할 수준의 안전성을 제공하는 암호 프로토콜에 대해서도 연구 진행중이다.

2. 양자암호의 안전성 증명과 도청방법

양자암호 이론 연구의 다른 한 축을 이루는 것은 양자암호에 대한 도청 방법 연구와 특정 양자 암호 프로토콜의 안전성 증명에 대한 연구이다. 안전성 증명은 크게 무조건 안전성과 실재적 안전성 두 가지로 나눌 수 있다. 무조건 안전성이란 도청자 Eve가 물리 법칙 내에서 모든 것을 할 수 있을 경우에도 두 사용자가 안전한 암호 키를 나누어 가질 수 있다는 것이다. 즉, 물리 법칙만이 도청자의 능력을 제한하는 상황에서도 안전한 통신이 가능함을 보이는 것이다. 보통 이러한 무조건 안전성의 증명은 수학적 정리의 형태를 띤다. 실재적 안전성의 증명은 보다 실험적 구현에 중점을 둔다.

Alice와 Bob이 양자암호통신을 구현하기 위해 사용한 장치들이 완벽하게 작동하는 경우에 양자암호의 안전성을 증명하는 문제는 간단하다. 반면, 그 장치들이 완벽하지 않은 경우 Eve는 그를 이용하여 암호 키에 대한 정보를 얻을 수 있다. 그러나, Eve가 키에 대해 가질 수 있는 정보량의 최대값이 Alice와 Bob 사이의 삼호정보량보다 적다면 Alice와 Bob은 고전적인 오류보정(error correction)과 비밀 종파

(privacy amplification)에 의해 안전한 비밀 키를 생성할 수 있다[12].

표준적인 BB84 프로토콜의 무조건적인 안전성의 증명은 1996년 D. Mayers에 의해 이루어졌다 [13]. 이 증명은 전송 채널과 광자 검출기에 잡음이 존재하며 광원은 완벽할 경우의 양자암호에 대한 것으로 POVM 모델을 사용하였다. 1999년 H.K. Lo 등은 잡음이 존재하는 양자계를 잡음이 없는 양자계로 환원한 후 이를 다시 잡음이 없는 고전계로 바꾸어 안전성을 증명했다[14]. 2000년에는 P. Shor와 J. Preskill이 모든 광원과 광검출기의 결점을 Eve의 기저에 무관한 공격에 포함된다고 가정하여 안전성을 증명하였으며, 이 증명은 흔히 Shor-Preskill 증명(Shor-Preskill proof)으로 알려져 있다. 2003년의 Koashi-Preskill 증명에서는 광검출기는 완전하다고 가정하고 광원이 Alice의 기저 정보를 Eve에게 흘려주진 않지만 완전하지는 않다는 가정을 하고 있다. D. Gottesman, H.K. Lo, N. Lutkenhaus, J. Preskill 등이 2004년 발표한 논문에서는 지금까지의 증명 중 실제 양자암호 시스템과 가장 유사하게 광원과 광검출기가 모두 기저에 대한 약간의 정보를 Eve에게 유출할 경우에 대한 안전성을 증명하였다[15].

실재적인 양자암호 시스템에서 특정한 양자암호 프로토콜을 제안할 경우나 실재적 안전성을 증명할 경우에는 Eve가 행할 수 있는 도청 방법을 상정해 두고 그 도청방법에 대해 안전함을 보이게 된다. Eve가 행할 수 있는 도청 방법은 크게 두 가지로 나눌 수 있는데 한 번에 하나의 큐빗에 대해서만 접근을 시도하는 개별 공격법(individual attack, incoherent attack)과 몇 개의 큐빗에 한꺼번에 접근하여 정보를 얻어내는 통합 공격법(joint attack, coherent attack)이 있다.

개별 공격법에 대한 분석에서는 모든 과정을 고전 확률론 문제로 변환 가능하므로 분석이 쉽게 된다. 가장 쉽게 생각할 수 있는 개별 공격법으로는 차단-재송신법(intercept-resend attack)을 들 수 있다. 이 방법은 말 그대로 Alice가 Bob에게 보내는

큐빗을 Eve가 기로채서 자신이 원하는 측정을 한 후 Bob에게는 Eve가 자신에게 유리한 상태의 큐빗을 보내는 방법이다. Eve가 측정하는 기저는 BB84 프로토콜의 두 기저 중에서 자신이 임의로 고를 수도 있고, 두 기저의 중간 기저로 측정할 수도 있다. 또 다른 개별 공격법에는 복제 공격법(cloning attack, symmetric individual attack)이 있다. 이는 전달되고 있는 큐빗에 양자 복제(quantum cloning)를 행하는 방법으로 양자 역학적으로 완전한 복제는 불가능하지만(no cloning theorem[5]) 암호 키에 대해 일부 정보를 얻는 형태의 공격이다.

이러한 공격 방법들은 완벽한 양자 암호 장치에 대한 공격이며 Alice와 Bob의 암호 키에 에러를 발생시켜 사용자에게 발각되는 것들이다. 이런 방법들 외에 양자암호 시스템에 사용되는 장치의 취약점을 이용하는 공격법도 있다. 특히 광원이 완벽한 단일 광자 상태를 만들어내지 못하고 일정 확률로 다중광자 상태를 내보내는 경우 이 다중광자 상태를 이용하는 양자 비파괴 공격법(quantum non-demolition attack)이 있다. 광자 수 나눔 공격(photon number splitting)이라고도 불리는 이 방법을 이용하면 전달되는 큐빗의 상태에 영향을 주지 않으면서 그 펄스에 포함된 광자의 개수는 측정이 가능함을 이용해서 다중광자 펄스 중 일부 광자를 나누어 가진 후 Alice와 Bob이 기저를 비교할 때 그 기저에 따라 측정함으로써 Alice와 Bob에게 발각되지 않으면서 비밀 키에 대한 완벽한 정보를 얻을 수 있다. 이러한 공격법에 대해서는 다중광자 상태를 만들어내기 위해 확률을 특정 기준 이하로 유지함으로써 대처할 수 있으며, 세 이상의 경로를 통한 위상 차이를 이용하거나, 위장용 펄스를 사용하는 등 프로토콜 자체에 변화를 줌으로써 대처하는 방법도 보고되고 있다.

그 외에도 특정 형태의 양자암호통신 시스템에 대한 공격법으로 뒤에서 설명할 “plug and play” 형태의 양자암호통신 시스템[16]에 대한 트로이의 목마 공격(Trojan horse attack)도 가능하다. 이 방법은 Alice가 Bob으로부터 받은 큐빗에 원하는 연산

을 수행한 후 되돌려 보내는 방식인 plug and play 양자 암호 시스템에서 Eve가 스파이 펄스를 Alice에게 보냄으로써 Alice쪽 실험 장치의 상태를 알아내는 것이다. 이에 대한 대처방법으로는 Alice가 자신에게 들어오는 광 펄스의 세기를 항상 분석하여 Eve의 존재를 확인하는 방법이 제안되고 있다[17].

III. 양자암호통신 구현기술

앞에서 설명한 BB84 프로토콜에서 보는 바와 같이 양자암호통신 기술은 양자상태를 “직접적으로” 암호 키 생성에 이용하는 것으로서 원리적으로 단일 양자(single quantum)의 복제 불가능성[5]에 기초하고 있다. 따라서 양자암호통신의 구현을 위해서는 단일광자(single photon) 상태와 같은 특별한 양자 상태의 빛을 사용해야 하며, 이러한 빛을 측정하기 위한 고감도 광자 검출기가 필수적이다. 또한, 광섬유 등을 이용하는 양자암호 통신채널 구현 시에도 사용하는 구체적인 코딩방식에 따라 특별한 구성방법이 필요하다. 본 절에서는 양자암호통신의 실제적인 구현과 관련된 양자광원 기술, 광자 검출기 기술, 그리고 양자암호통신 채널의 구성방법 등에 대한 기본 개념과 최근의 연구개발 동향을 기술한다.

1. 양자광원

앞에서 기술한 BB84 프로토콜을 포함한 많은 양자암호 프로토콜들은 단일광자 상태를 사용하는 방식으로서 단일광자 상태는 양자암호통신에서 특별히 중요하다. 이상적인 단일광자 상태는 정해진 하나의 모드에 오직 한 개의 광자만이 존재하는 상태를 말한다. 이러한 단일광자 상태는 두 가지 에너지 준위만을 가지는 고립된 원자 한 개를 여기시켰을 때 그 원자에서 방출되는 형광(fluorescence)으로부터 얻을 수 있다. 따라서 만약 광자검출기의 측정 분해시간보다 짧은 시간간격 동안에 더 이상 그 원자를 여기시키지 않는다면 두번째 광자가 원자로부터 방출될 확률은 없으므로 광자검출기는 오직 한

번에 한 개의 광자만을 측정하게 된다. 통계적으로 실제 단일광자 상태는 가변도(variance)가 평균값 보다 작아서 측정된 광자 수의 분포가 상대적으로 좁게 되는 아포아송(sub-Poisson) 분포를 보이게 되며, 빔 분할기(beam splitter)와 두 개의 광자검출기를 이용하여 동시에 두 개의 광자를 측정하는 상관관계 측정에서는 광자 홀어짐(photon antibunching) 효과가 나타나게 된다. 현재까지 실험적으로 구현된 단일광자 광원들은 단일분자를 제한적으로 여기시키는 방법[18], 다이아몬드 결정구조에 질소 원자 한 개를 치환해서 여기시키는 방법[19], 반도체 양자점을 이용하는 방법[20], 반도체 양자점에서 히향변환 과정에서 동시에 발생하는 광자쌍 중에서 하나의 광자를 측정했을 때 다른 광자가 단일광자 상태에 존재하게 되는 현상을 이용하는 조건부 단일광자 광원[22] 등이 있다. 그러나 상기의 어떤 방법도 현재 기술적으로 완전하지 못한 상태이며 낮은 광자 발생효율과 높은 잡음 광자 수 등 해결해야 할 기술적인 난제들로 인하여 실제 양자암호통신에 사용되기에에는 무리가 있다.

단일광자 상태를 만들기 위해서 생기는 여러 가지 실제적인 문제를 피하기 위해서 다른 대안으로 이용되는 것이 레이저 펄스를 아주 약하게 감쇄시켜서 유사 단일광자 상태를 만드는 방법이다. 이러한 유사 단일광자 상태는 그 통계적인 특성이 이상적인 단일광자 상태와는 다르며 포아송(Poisson) 분포를 따르게 되지만, 예를 들어 평균 광자 수가 0.1인 경우 한 번의 측정에서 한 개의 광자를 측정할 확률이 9% 정도인데 반해서 한 개의 펄스에서 두 개의 광자가 존재할 확률은 0.5% 정도로 낮아서 단일광자 상태를 사용하는 경우와 유사한 광자 통계를 나타내므로 실제 양자암호통신 구현실험에서 많이 이용되고 있다.

다른 한편, 최근 양자정보기술 분야에서 많이 사용되고 있고 앞으로도 여러 가지 측면에서 연구의 대상이 되고 있는 양자 얹힘상태(entangled state)를 양자암호통신의 광원으로 이용하는 방법도 많이

연구되고 있다. 얹힘상태는 양자역학의 가장 근본적인 특성 중의 하나로서, 둘 이상의 입자들이 서로 특별한 중첩된 상태에 있어서 그 전체 상태가 개별적인 입자들의 파동함수의 곱으로 기술할 수 없는 양자상태를 말한다. 특히 두 입자 얹힘상태의 대표적인 예로는 D. Bohm이 제안한 스핀이 1/2인 한 쌍의 전자 사이에 존재하는 스핀의 비대칭 상관관계와 두 전자의 스핀상태의 중첩, 즉

$$|\Psi\rangle = \frac{1}{\sqrt{2}} (| \uparrow_1 \downarrow_2 \rangle - | \downarrow_1 \uparrow_2 \rangle) \quad (1)$$

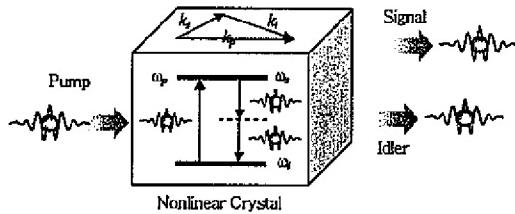
식 (1)같이 표현되는 상태이다[23]. 공간적으로 서로 멀리 떨어져 있는 두 입자 1과 2는 스핀-up (\uparrow)의 상태와 스핀-down (\downarrow)의 상태가 서로 중첩된 상태에 있으며, 한 입자의 스핀이 측정을 통해 특정한 방향으로 결정됨과 동시에 다른 입자의 스핀은 자동적으로 반대 방향으로 결정되게 된다.

이러한 양자 얹힘상태를 생성하기 위해서 1980년대 중반까지는 주로 원자의 단단천이(atomic cascade) 현상이 이용되었지만[24], 1980년대 후반부터는 자발적인 매개하향변환(SPDC) 과정[25]에서 발생하는 광자쌍을 이용해서 얹힘상태를 만드는 것이 가장 보편적인 방법으로 정착되고 그 후 양자암호통신 및 양자컴퓨팅의 구현연구에 광범위하게 사용되고 있다.

SPDC는 높은 진동수(또는 짧은 파장)의 레이저 광을 $x^{(2)}$ 의 비선형 계수를 갖는 매질에 입사시킬 때 입사하는 광자의 일부가 상대적으로 낮은 진동수(또는 긴 파장)를 갖는 한 쌍의 광자들로 자발적으로 변환되는 과정을 말한다. 관례적으로 매질에 입사하는 빛을 펌프광, 상호작용에 의해 발생하는 두 광자를 signal 광자와 idler 광자라고 부른다. SPDC는 비선형 매질 내에서 펌프 광자와 하향 변환된 광자들 사이에 에너지 보존법칙과 운동량 보존법칙이 만족될 때 효과적으로 일어난다(식 (2)).

$$\omega_p = \omega_s + \omega_i, \quad k_p = k_s + k_i \quad (2)$$

즉, (그림 2)에서 보는 바와 같이 SPDC에서 발생하는 두 개의 광자들의 진동수(또는 파장)와 운동량



(그림 2) 자발적 매개하향 변환과정

이 서로 상관되어 있으므로 signal 광자가 임의의 진동수와 파수 벡터를 갖고 발생하면 이에 대응하는 진동수와 파수 벡터를 가지는 idler 광자 한 개가 반드시 발생하게 된다.

SPDC 과정은 발생한 두 광자의 편광이 동일한 상태에 있는 제1형(type-I)과 두 광자의 편광이 서로 직교하는 제2형(type-II)이 있으며, 이러한 광자 쌍 발생방식과 간섭계를 구성하는 방법에 따라서 다양한 형태의 양자 얹힘상태를 구현할 수 있다. 예를 들어 SPDC 과정에서 발생하는 두 광자의 진동수를 서로 다르게 선택할 경우

$$|\Psi\rangle = \frac{1}{\sqrt{2}} (| \omega_1 \rangle | \omega_2 \rangle + | \omega_2 \rangle | \omega_1 \rangle) \quad (3)$$

(3)과 같이 진동수 얹힘 상태(frequency-entangled state)를 구현할 수 있으며, 또한 제2형 SPDC 과정을 이용해서 서로 다른 편광의 광자쌍을 발생시킬 경우에는

$$|\Psi\rangle = \frac{1}{\sqrt{2}} (| H \rangle | V \rangle + | V \rangle | H \rangle) \quad (4)$$

(4)와 같이 수평편광(H)과 수직편광(V)이 중첩된 편광 얹힘상태(polarization-entangled state)를 구현할 수 있다[26]. 한편 각각의 광자가 서로 다른 간섭계의 짧은 경로(s)와 상대적으로 긴 경로(l)를 선택할 수 있게 간섭계를 구성하면

$$|\Psi\rangle = \frac{1}{\sqrt{2}} (| s \rangle | l \rangle + | l \rangle | s \rangle) \quad (5)$$

(5)의 형태로 표현되는 energy-time 얹힘상태 또는 이의 팔스모드 형태인 time-bin 얹힘상태를 구현할 수도 있다[27].

이와 같이 SPDC 과정에서 생성되는 광자쌍의 발생방식과 간섭계의 구성방법에 따라서 다양한 형태의 양자얽힘상태를 손쉽게 만들 수 있으므로 최근 이러한 광자쌍 양자얽힘상태를 이용한 양자암호통신 구현연구가 활발하게 진행되고 있다[28]~[30].

2. 광자검출기

양자암호통신 기술의 실제 구현을 위해서는 고성능의 광자검출기가 필수적이다[31]. 특히, 광섬유나 대기 중을 통해서 단일광자 수준의 광 신호를 전송할 경우 발생하는 광 손실은 거리에 비례해서 증가하며 따라서 광자검출기의 양자효율(광자 한 개가 입사할 경우의 검출효율)은 양자암호의 통신거리를 제한하는 주요 인자가 된다. 또한, 광자검출기의 양자효율과 잡음(dark noise) 수준은 양자암호통신의 에러율과 직접적으로 관련되므로 높은 양자효율과 낮은 잡음수준을 갖는 광자검출기는 양자암호통신 시스템의 성능을 좌우하는 핵심적인 사항이다.

기존의 광통신기술에서 사용하는 PIN 타입의 광검출기는 고속으로 동작하는 장점이 있지만 양자효율이 단일광자 수준의 광을 검출하기에는 지나치게 낮으므로 양자암호통신에서는 주로 APD 타입의 광검출기를 사용한다. 그러나, APD는 일반적으로 광검출 시에 응답속도가 느리므로(dead time) 고속으로 동작하지 못하는 단점이 있어서 수 MHz 이상으로 동작하기에는 무리가 있다. 그러나 이러한 단점에도 불구하고 APD 타입의 광 검출기는 현재 양자암호통신에서 사용할 수 있는 최선의 선택으로 생각된다.

양자암호통신에서 사용하는 빛은 광 펄스 당 0.1 개 정도의 광자가 존재하는 극히 낮은 세기의 빛이므로 양자효율을 높이기 위해서 APD에 인가하는 바이어스전압을 breakdown 전압보다 높게 사용하는 소위 “Geiger mode”에서 동작하는 것이 일반적이다. 이 경우 한 번의 광자검출 전류신호가 지나치게 방전되는 것을 막기 위해서 “quenching circuit”을 사용한다. 500~900nm 대역에서 주로 사용하는

Si APD 타입의 광자검출기는 양자효율이 60~70%에 이르는 고성능 제품들이 상품화 되어 있다. 이러한 제품에서는 동작속도를 높이기 위해서 보통 “active quenching circuit”을 채용하고 있다. 그러나, 통신파장 영역인 1310nm나 1550nm 대역에서 주로 사용하는 InGaAs APD 타입의 광자검출기는 잡음지수가 매우 높은 관계로 quenching 모드에서 동작시키기가 매우 어려우며 따라서 수 나노 초 정도의 아주 좁은 시간간격 동안만 바이어스전압을 인가하는 소위 “gated-Geiger mode”에서 동작시키는 것이 일반적이다. 이 경우 광자의 도달시각과 게이트 전압 인가 시각이 정확히 일치해야 하므로 quenching mode와 비교해서 사용이 어려운 단점이 있다. 현재 사용되고 있는 InGaAs APD 타입의 광자검출기는 gated-Geiger mode에서 잡음 광자 검출확률이 $10^{-6}/\text{ns}$, 양자효율이 10% 정도인 것이 일반적이다. 또한, 일부 연구자들이 양자효율 20~30%대의 InGaAs APD 타입 광자검출기를 보고하고 있으나 이 경우 잡음 광자 검출확률도 함께 증가하는 것이 보통이며 사용하는 InGaAs APD의 성능에 좌우되는 면이 크다. 현재 700nm 대역에서 Si APD 타입의 광자검출기가 보여주는 정도의 고성능으로 통신파장대역에서 동작하는 InGaAs APD 타입 광자검출기를 개발하기 위한 연구개발 노력이 계속되고 있다[31].

한편, 앞에서 설명한 광자검출기 외에 입사하는 빛의 광자 개수를 분해할 수 있는 광자검출기나 비선형광학적인 방법을 사용하여 입사하는 빛의 파장을 변환하여 광자검출을 함으로써 양자효율을 개선하는 방법 등 새로운 시도들이 진행중에 있다.

3. 양자암호통신 채널

양자암호 혹은 양자 키 분배 기술은 멀리 떨어진 두 사용자(Alice와 Bob) 사이에 양자역학적으로 완벽한 보안성이 보장되는 비밀 키를 분배하는 기술로서 본질적으로 통신네트워크의 물리계층 보안 기술이다. BB84 프로토콜에서 보듯이 일반적으로 양자

암호통신에서는 양자상태를 전송하는 양자채널(비밀채널)과 도청자를 포함한 외부에 완전히 공개된 고전채널(공개채널)의 두 가지 통신채널을 사용한다. 즉, 양자채널은 양자암호통신의 핵심이 되는 통신채널로서 양자 복제불가능 원리에 의해서 완전히 비밀이 유지되는 반면, 고전채널은 Alice와 Bob이 무작위로 선택한 기저를 공개적으로 서로 비교하거나 혹은 생성된 암호 키의 일부분을 서로 공개적으로 비교해서 도청자를 탐지하기 위해 사용하는 통신채널로서 기존의 디지털 광전송 채널이나 무선통신 채널을 말한다. 양자암호통신에서 고전채널은 원칙적으로 도청자가 자유롭게 도청이나 감청을 할 수 있는 채널로 간주한다. 고전채널은 Alice와 Bob이 서로의 기저를 비교하는 등 양자암호 키 분배 자체를 위해서도 필요하지만 다른 한편 서로 상대방을 공개적으로 인증(authentication)하는 기능을 위해서도 반드시 필요하다. 즉, 고전채널이 없을 경우에는 도청자가 중간에서 Alice나 Bob의 흉내를 내는 소위 “분장공격(impersonation attack)”에 의해서 암호 키가 유출될 수 있다. 이와 같이 고전채널 혹은 공개채널은 양자암호통신의 핵심요소로서 실제적인 양자암호통신 시스템 구현 시 중요하게 고려되어야 하지만 기존의 개발된 기술을 사용한다는 점에서 본고에서는 더 이상 논의하지 않으며 본고에서 말하는 양자암호통신 채널은 양자상태 전송에 사용되는 양자채널에 국한한다.

1984년 Bennett과 Brassard가 제안한 BB84 양자암호 프로토콜은 1989년 Bennett 등에 의해 처음으로 실험으로 증명되었고 1992년 그 결과가 발표되었다[6], [32]. 그 이후로 지금까지 양자 키 분배 기술은 전 세계적으로 많은 실험적 구현연구가 이루어졌으며 몇몇 연구 그룹은 실제 실험실 밖 환경에서 테스트 한 결과를 발표하기도 했다[33], [34]. <표 1>은 지금까지 발표된 대표적인 실험연구 결과들이다.

양자암호 통신채널을 물리적으로 구현하는 방식에는 광섬유를 사용하는 방식(유선)과 대기 중을 통해서 암호 키를 분배하는 방식(무선)의 두 가지가 있

다. 두 가지 방식은 서로 원리적으로 차이가 없으나 대기와 광섬유의 물리적인 특성이 다르므로 사용하는 빛의 파장대역 및 응용분야도 서로 다르다.

대기 중을 통한 양자암호통신에서는 770nm 대역의 빛에서 투과손실이 적으며 또한 이 파장대역에서 Si APD 광자검출기의 양자효율도 60~70% 정도로 높은 성능을 보이므로 주로 이 파장대역을 이용해서 통신채널을 구성한다. 대기 중을 통한 양자암호통신은 특히 위성과 지상 사이의 암호통신에 응용 가능하다는 것이 큰 장점이다. 그러나, 대기 중을 통한 양자암호통신 채널에서는 거리가 늘어남에 따라 빔이 공간적으로 퍼지는 문제와 날씨 등의 영향이 심각하므로 주로 단거리 암호통신에 그 응용이 제한된다. 현재 대기 중을 통한 암호통신은 23.4km 통신거리에서 수백 bps 정도의 키 생성실험이 보고되고 있다(<표 1> 참조).

한편, 광섬유를 이용하는 방식은 기존의 광통신에서 표준적으로 사용되고 있는 단일모드 광섬유를 사용하면 공간적인 모드가 아주 잘 유지되며 또한 1550nm 대역에서 투과손실이 0.2dB/km 정도로 아주 낮으므로 장거리 양자암호채널 구현에 적합하다. 그러나 광섬유를 통한 광자 전송 시에 발생하는 분산(dispersion), 편광의 변화, PMD, 기타 다양한 비선형 효과들은 양자암호통신 시스템의 성능을 떨어뜨리게 된다[3]. 현재 광섬유 전송 시에 발생하는 이러한 문제를 극복하기 위한 다양한 연구가 진행되고 있으며, 67km 광섬유 채널을 통해서 수십 bps 정도의 양자 암호 키 생성 실험이 보고되고 있다(<표 1> 참조).

양자암호통신의 암호 키는 빛의 편광을 이용해서 코딩하거나 위상 코딩, 주파수 코딩, 연속변수를 이용한 코딩 등 다양한 방식으로 구현이 가능하다. 빛의 편광이나 위상을 이용한 코딩 기술은 온도나 주위 환경 등에 의해서 편광이나 광학적 경로의 혼들림이 발생하므로 이를 연속적으로 보상하기 위한 기술이 부가적으로 요구된다. 최근, 광섬유를 통한 양자 키 분배 시에 발생하는 편광의 변화나 경로의 혼들림을 능동 소자를 사용하지 않고 패러데이 거울

〈표 1〉 주요 양자암호 실험 현황

연구기관	국가	기술내용	성능			발표 년도	참고문헌	비고
			키 생성속도	거리	QBER			
IBM(C.H. Bennett)	미국	Free air channel Polarization coding	10bps	30cm	-	1992	J. Cryptology, vol.5, p.3	최초의 양자 암호 실험
BT Lab.(P. Townsend)	영국	Multi-user, 1X3 PON system	1kbps	5.4km	3%	1997	Nature, vol.385, p.47	다중 사용자, PON 구조
Los Alamos Lab. (R. Hughes, C.G. Peterson)	미국	Double Mach-Zehnder type Installed fiber channel	10bps	48km	9.3%	2000	J. Mod. Opt., vol.47, p.533	
Universität Wien (A. Zeilinger)	오스트리아	Entangled photon pairs Polarization coding 700nm fiber channel	420bps	500m	3.4%	2000	Phys. Rev. Lett. vol.84, p.4729	
University of Geneva (N. Gisin)	스위스	Entangled photon pair energy-time coding 1310nm fiber channel	33bps	20km	4%	2000	Phys. Rev. Lett. vol.84, p.4737	
Heriot-Watt University (G. Buller), Comming Research Centre(P. Townsend)	영국	Spatial multiplexing 1550nm fiber channel	-	80km	9%	2001	J. Mod. Opt., vol.48, p.1957	
Defence Evaluation and Research Agency(J. Rarity, P. Gorman, P. Tapster)	영국	Polarization coding free space channel	685bps	1.9km	5.1%	2001	Elec. Lett. vol.37, p.512	
University of Geneva (N. Gisin)	스위스	Plug & Play system 1550nm fiber channel	44bps	67.1km	6.1%	2002	New J. Phys. vol.4, p.41	Plug & Play
Mitsubishi Electric	일본	1550nm fiber channel between Tokyo and Mt. Fuji	7.2bps	87km	7.6%	2002	Mitsubishi Electric Report	
Ludwig-Maximilian University(H. Weinfurter)	독일	Polarization coding Free space channel	hundreds bps	23.4km	-	2002	Nature vol.419, p.450	
Los Alamos Lab. (R. Hughes, C.G. Peterson)	미국	Free air channel in daylight Polarization coding	651bps	10km	3.2%	2002	New J. Phys. vol.4, p.43	
IBM(D. Bethune, W. Risk)	미국	Autocompensating type Phase coding	200bps	20km	3%	2002	New J. Phys. vol.4, p.42	
BBN, Harvard, Boston University(G. Troxel)	미국	Quantum Network Standard telecom fiber	1kbps	10km	6~8%	2003	quant-ph/0307049 IEEE	VPN 기반 테스트베드 구축
Tekcordia Technologies (M. Goodman), Los Alamos Lab.(R. Hughes)	미국	1300nm data signal 1550nm sync signal	91bps	10km	-	2003	Photronics Tech. Lett. vol.15, p.1669	
I'Institut d'Optique (P. Grangier), Université Libre de Brux(N. Cerf)	프랑스 벨기에	Continuous variable QKD	470kbps	tabletop	-	2003	Nature, vol.421, p.238	연속변수 이용
Toshiba Research Europe (A.J. Shields)	영국	Plug & Play system 1550nm fiber channel	9.2bps	122km	8.9%	2004	App. Phys. Lett. vol.84, p.3762	
NEC, ERATO (K. Nakamura)	일본	PNP system 1550nm fiber channel	-	150km	-	2004	Jpn. J. Appl. Phys. vol.43, L1217	단순한 간섭 현상 확인 실험
NIST(C.J. Williams)	미국	845nm free space channel, 1.25Gbps clock sync.	1Mbps	730m	1.1%	2004	Opt. Express, vol.12, p.2011	

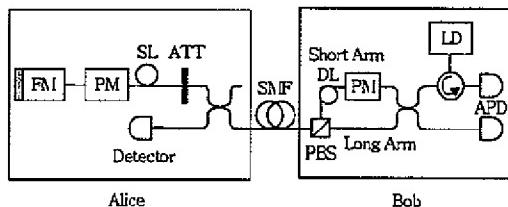
(뒤에 계속)

(계속)

연구기관	국가	기술내용	성능			발표년도	참고문헌	비고
			키 생성속도	거리	QBER			
University of Geneva (N. Gisin)	스위스	Energy-time entanglement Standard telecom fiber	23bps	30km	10.5%	2004	Eur. Phys. J. D, vol.30, p.143	양자 얹힘 광원
Heriot-Watt University (G. Buller)	영국	Polarization coding B92					IEEE J. Q. Elec. vol.40, p.900	
University College Cork (P. Townsend)	아일랜드	1300nm fiber channel GHz clocked	7kbps	10km	2.1%	2004		
Northwestern University (H.P. Yuen, P. Kumar)	미국	Coherent state의 양자 잡음을 이용하는 방법, Yuen protocol	650Mbps	200km	-	2005	Phys. Rev. vol.71, p.062326	프로토콜의 안전성 미검증
NTT, Stanford University (Y. Yamamoto)	일본 미국	Differential phase shift QKD	209bps	105km	7.95%	2005	quant-ph/0507110	DPSK 방법

(faraday mirror)을 이용하여 자동적으로 보상하는 소위 “plug and play 양자암호 기술”이 스위스 제네바대학교의 Nicolas Gisin 교수 등에 의해 개발되었다[16], [35]. (그림 3)은 plug and play 양자암호 시스템의 구성도이다.

Plug and play 양자암호 시스템의 동작원리는 다음과 같다. 먼저 Bob측에서 방출되는 강한 레이저 펄스(1550nm)는 빔 분할기(beam splitter)에 의해 50/50으로 분할된다. 분할된 이 두 펄스들은 각각 짧은 경로와 광 위상변조기(phase modulator)와 광 지연선(delay line)을 갖는 긴 경로를 거친 후 편광 분할기(PBS)의 한 쪽 출력 포트로 나오게 된다. 편광 분할기로 출력된 펄스들은 서로 수직한 편광 성분을 가지며 광학적 지연에 의해 시간축 상에서 분리되어 있다. 이 펄스들은 Alice에게 전송되어 광 감쇠기에 의해 단일광자 수준의 세기로 감쇄되고 패러데이 거울에 의해 입사 편광의 수직한 편광 성분으로 바뀌어 다시 Bob에게 돌아오게 된다. 돌아온 이 두 펄스들은 Bob측의 간섭계에서 원래의 경로와 다른 경로를 거치게 되며 빔 분할기에 동시에 도착하여 간섭이 생기게 된다. 즉, 두 펄스들은 패러데이 거울에 의해 자동적으로 같은 경로의 길이를 지나게 되며 또한, 진행할 때와 반사되어 돌아올 때 편광이 서로 수직이므로 광섬유상에서 광 펄스가 겪는 복굴절로 인한 비선택형 효과가 서로 상쇄되어 안정적인 간



(그림 3) Plug and Play 양자암호시스템의 구성도

섭을 일으키게 되는 것이다. 그리고, 암호 키는 Bob에서 Alice로 갔다가 돌아오는 광 펄스들의 위상에 코딩된다. 예를 들어, BB84 프로토콜을 구현하기 위해서 Alice측 위상 변조기를 통과하는 두번째 펄스에 0 혹은 π 그리고 $\pi/2$ 혹은 $3\pi/2$ 를 임의로 인가하고 Bob은 돌아오는 첫번째 펄스에 0 혹은 $\pi/2$ 를 인가하면 된다.

이러한 plug and play 타입 양자암호기술은 광섬유를 통한 장거리 전송에 적합하며 많은 연구 그룹들이 실제 구현연구를 진행해 온 대표적인 양자암호 구현 기술이다. 그러나 기본적으로 양방향 통신 방식이므로 광 펄스가 진행할 때 생기는 레일라이 산란(Rayleigh backscattering)에 의한 에러가 심각하며 양자암호통신의 성능을 저하시키는 주요 원인이 된다. 양자암호통신 채널을 구현하는 기술은 상기의 plug and play 기술 이외에도 매우 다양하며 현재 각 방식의 단점들을 개선하기 위한 여러 가지 새로운 시도들이 계속되고 있다[3].

IV. 결론

지금까지 새로운 차세대 통신보안기술로 주목을 받고 있는 양자암호통신의 기본동작원리와 제반 구현기술 및 기술개발 동향에 대해서 살펴보았다. 특히, 최근 들어서 통신상의 보안문제가 기술적인 측면뿐만 아니라 정치, 경제, 사회적으로 점점 더 그 중요성이 더해가고 있으며, 따라서 절대적인 보안성을 제공하는 양자암호통신 기술개발과 상용화에 대한 관심도 더욱 커지고 있다.

양자암호통신 기술은 원리적인 측면에서는 앞에서 설명한 BB84, B92, E91 등의 프로토콜에 기초하고 있으며 이러한 기초적인 원리들은 실험을 통해서 이미 상당부분 증명이 완료되었다. 그러나, 이 기술의 실제 구현 및 상용화를 위해서는 아직도 해결해야 할 많은 기술적인 난제들이 있다. 먼저 프로토콜 분야에서는 기본적인 BB84 등의 프로토콜을 실제 구현에 적합하게 개선하거나 혹은 실제 실험 장치들의 한계를 고려한 새로운 프로토콜의 연구 등이 필요하다. 구현기술 분야에서는 전송거리 확대와 암호 키 생성 속도의 증대, 그리고 완벽한 프로토콜 구현을 위해서 진정한 의미의 단일광자 광원 및 고효율 양자광원 개발, 고성능 광자검출기 개발, 양자 중계기 개발 및 더욱 효과적인 시스템 구도 개발 등이 필요하다. 양자암호통신 시스템의 상용화를 위해서 해결해야 할 또 다른 기술적인 문제들로는 시스템의 안정성 확보와 기존 네트워크와의 정합기술개발 등이 있다. 그리고 통신 사업자들이나 네트워크 사용자의 관점에서 경제성을 확보하기 위해서는 현재의 기술수준을 메트로급 네트워크에 적용 가능한 수준으로 발전시켜야 할 것으로 보인다.

양자암호통신 시스템의 상용화 시점에서 그 응용분야는 우선적으로 절대 보안이 필수적인 국방, 금융 등 핵심 기간 통신망이 될 것이며, 그 첫 단계는 point-to-point 양자암호통신부터 시작하여 궁극적으로는 point-to-multipoint 양자암호네트워크 연결로 그 응용이 확대될 것이 분명하다. 기술의 특성상 암호관련 기술은 외국으로부터 도입하기가 매우

어려우며 국가 안보와 관련된 극히 중요한 기술이므로 미래 통신산업 경쟁력 확보뿐만 아니라 우리나라의 국가 정보보안 주권 확립의 차원에서도 양자암호통신 관련 기술의 개발이 절실하다.

약어 정리

APD	Avalanche Photodiode
DL	Delay Line
EPR	Einstein-Podolsky-Rosen
FM	Faraday Rotator Mirror
LD	Laser Diode
PBS	Polarization Beam Splitter
PM	Phase Modulator
PMD	Polarization Mode Dispersion
POVM	Positive Operator Valued Measurement
QKD	Quantum Key Distribution
Qubit	Quantum Bit
RSA	Rivest, Shamir, Adleman
SL	Storage Line
SPDC	Spontaneous Parametric Down-Conversion

참 고 문 헌

- [1] J.L. Massey, "An Introduction to Contemporary Cryptography," *Proc. of the IEEE*, Vol.76, No.5, 1988, p.633.
- [2] P. Shor, in *Proc. of the 35th Annu. Symp. on Foundations of Computer Science*, edited by S. Goldwasser, IEEE Computer Society Press, Los Alamitos, California, 1994, pp.124.
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Rev. Mod. Phys.*, Vol.74, No.1, 2002, p.145.
- [4] C.H. Bennett and D. DiVicenzo, "Quantum Information and Computation," *Nature*, Vol.404, 2000, p.247.
- [5] W.K. Wootters and W.H. Zurek, "A Single Quantum Cannot be Cloned," *Nature*, Vol.299, 1982, p.802.
- [6] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proc. of IEEE Int'l Conf. on Computers, Systems*

- and Signal Proc., Bangalore, India, IEEE, New York, 1984, p.175.
- [7] C.H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States" *Phys. Rev. Lett.*, Vol.68, 1992, p.3121.
- [8] J.M. Renes, "Spherical-code Key-distribution Protocols for Qubits," *Phys. Rev. A* 70, 052314, 2004.
- [9] A.K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Phys. Rev. Lett.*, Vol.67, 1991, p.661.
- [10] C.H. Bennett, G. Brassard, and N.D. Mermin, "Quantum Cryptography without Bell's Theorem," *Phys. Rev. Lett.*, Vol.68, 1992, p.557.
- [11] F. Grosshans, G.V. Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, "Quantum Key Distribution Using Gaussian-modulated Coherent States," *Nature*, Vol.412, 2003, p.238.
- [12] N. Lütkenhaus, "Security Against Eavesdropping in Quantum Cryptography," *Phys. Rev. A* 54, 1996, p.97.
- [13] D. Mayers, "Quantum Key Distribution and String Oblivious Transfer in Noisy Channels," in *Advances in Cryptography-Proc. of Crypto'96*, Lecture Notes in Computer Science, Vol.1109, pp.343-357, edited by N. Koblitz, Springer-Verlag, New York, 1996.
- [14] H.K. Lo and H.F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science*, Vol.283, 1999, p.2050.
- [15] D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill, "Security of Quantum Key Distribution with Imperfect Devices," *Quantum Inf. Comput.*, Vol.4, 2004, p.325.
- [16] A. Müller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and Play Systems for Quantum Cryptography," *Appl. Phys. Lett.*, Vol.70, 1997, p.793.
- [17] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan Horse Attacks on Quantum Key Distribution Systems," quant-ph/0507063, 2005.
- [18] B. Lounis and W.E. Moerner, "Single Photons on Demand from a Single Molecule at Room Temperature," *Nature*, Vol.407, 2000, p.491.
- [19] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, "Stable Solid-state Source of Single Photons," *Phys. Rev. Lett.*, Vol.85, 2000, p.290.
- [20] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, "A Single-photon Turnstile Device," *Nature*, Vol.397, 1999, p.500.
- [21] E. Moreau, I. Robert, J.M. Gérard, I. Abram, L. Manin, and V. Thierry-Mieg, "Single-mode Solid-State Single Photon Source Based on Isolated Quantum Dots in Pillar Microcavities," *Appl. Phys. Lett.*, Vol.79, 2001, p.2865.
- [22] A.L. Migdall, D.A. Branning, S. Castelletto, and M. Ware, "Single Photon Source with Individualized Single Photon Certifications," *Free-Space Laser Communication and Laser Imaging II: Proc. the SPIE - The International Society for Optical Engineering*, Vol.4821, 2002, p.455.
- [23] D. Bohm, *Quantum Theory*, Prentice-Hall, New York, 1951.
- [24] A. Aspect, P. Grangier, and G. Roger, "Experimental Tests of Realistic Local Theories via Bell's Theorem," *Phys. Rev. Lett.*, Vol.47, 1981, p.460.
- [25] D.C. Burnham and D.L. Weinberg, "Observation of Simultaneity in Parametric Production of Optical Photon Pairs," *Phys. Rev. Lett.*, Vol.25, 1970, p.84.
- [26] P.G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, "New High-Intensity Source of Polarization-Entangled Photon Pairs," *Phys. Rev. Lett.*, Vol.75, 1995, p.4337.
- [27] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, "Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication," *Phys. Rev. Lett.*, Vol.82, 1999, p.2594.
- [28] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum Cryptography with Entangled Photons," *Phys. Rev. Lett.*, Vol.84, 2000, p.4729.
- [29] D. Naik, C. Peterson, A. White, A. Berglund, and P. Kwiat, "Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol," *Phys. Rev. Lett.*, Vol.84, 2000, p.4733.
- [30] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum Cryptography Using Entangled Photons in Energy-Time Bell States," *Phys. Rev. Lett.*, Vol.84, 2000, p.4737.
- [31] Journal of Modern Optics, Special Issue on Single-photon: Detectors, Applications, and Measurement methods, edited by A. Migdall and J. Dowling, *J. Mod. Opt.*, Vol.51, No.9-10, 2004, pp.1265-1557.

- [32] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," *J. Cryptology*, Vol.5, No.3, 1992.
- [33] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum Key Distribution over 67km with a Plug & Play System," *New J. of Physics*, Vol.4, 41.1, 2002.
- [34] D. Bethune and W. Risk, "An Auto-compensating Fiber-optic Quantum Cryptography System Based on Polarization Splitting of Light," *IEEE J. Quantum Electron.*, Vol.36, 2000, p.340.
- [35] G. Ribordy, J.D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Automated 'Plug & Play' Quantum Key Distribution," *Electron. Lett.*, Vol.34, 1998, p.2116.